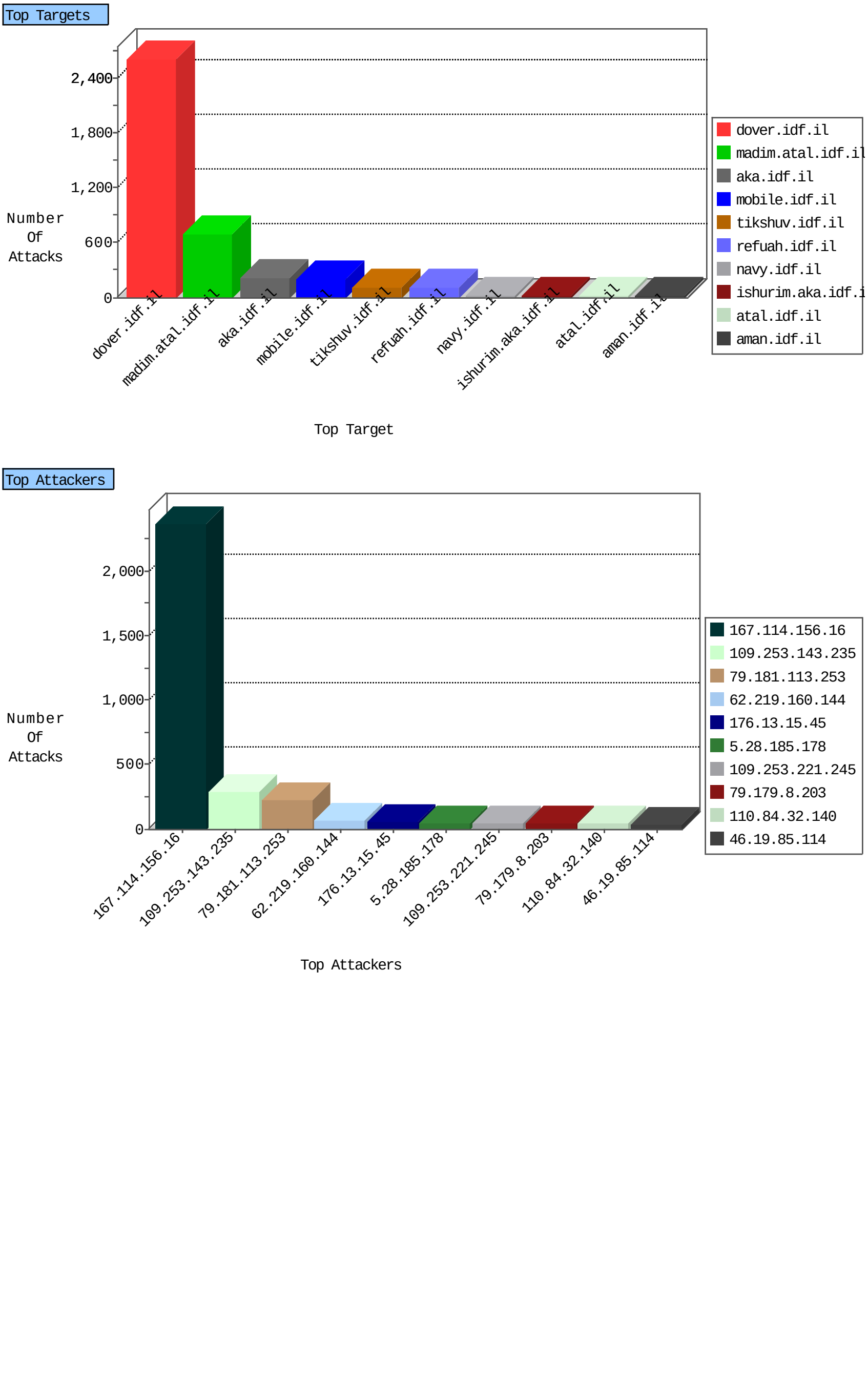
01-21-2016-13:04:09 to 01-21-2016-14:04:09

IDF Under Attack Daily Report



01-21-2016-13:04:09 to 01-21-2016-14:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3076
109.67.173.105	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	24
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	4
74.91.28.60	United States	147.237.77.235	sviva.idf.il	block-sp-traf1	drop	1
142.54.169.165	United States	147.237.77.74	law.idf.il	block-sp-traf1	drop	1
74.91.28.61	United States	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1
142.54.160.211	United States	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	forward	1

01-21-2016-13:04:09 to 01-21-2016-14:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-21-2016-13:04:09 to 01-21-2016-14:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
5.28.142.197	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.132.53.179	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
91.218.246.103	147.237.8.46	Russian Federation	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
84.94.70.224	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
37.26.149.253	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.52.6.70	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
91.218.246.103	147.237.8.27	Russian Federation	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1

01-21-2016-13:04:09 to 01-21-2016-14:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
62.219.160.144	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	62
79.179.8.203	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
109.253.221.245	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
2.54.37.42	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.19.85.252	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
82.145.208.23	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
46.19.85.228	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
81.218.163.134	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
185.32.179.105	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.146.197	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	11
46.19.85.51	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
5.102.254.15	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
185.120.126.29		147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
80.246.140.86	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.147.201	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.157	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
94.230.86.235	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
188.120.148.227	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
81.218.198.179	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.153	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
89.138.93.75	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.181.113.253	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.149	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.153	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
207.46.13.2	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.51	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
176.13.11.11	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.157	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
84.109.124.3	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.142.186.39	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.157	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
31.210.187.139	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
84.108.171.82	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.121.142.2	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
79.178.109.158	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
84.108.70.99	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.186.237	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
66.249.66.93	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
84.228.201.70	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
192.114.105.254	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
84.108.171.82	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
37.46.39.31	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
84.228.201.70	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.180.14.240	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.230.86.235	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
188.120.148.183	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.143.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	148
109.253.143.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	139
79.181.113.253	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	108
79.181.113.253	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	93
176.13.15.45	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.15.45	Block	58
5.28.185.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	53
46.19.85.114	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	37
46.19.85.38	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
37.26.147.249	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	23
109.253.146.216	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
37.26.147.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	17
37.142.68.82	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 37.142.68.82	Block	17
79.181.113.253	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	16
109.253.221.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
110.84.32.140	China	147.237.76.147	chinuch.aka.idf.i	Multiple Unauthorized URL Access from 110.84.32.140	Block	14
79.179.8.203	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	10
2.52.165.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
110.84.32.140	China	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 110.84.32.140	Block	10
110.84.32.140	China	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 110.84.32.140	Block	8
109.253.221.245	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
110.84.32.140	China	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 110.84.32.140	Block	4
46.19.85.252	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
46.19.86.226	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.207.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.37.42	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.228	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
80.246.137.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.147.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
5.22.135.136	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	3
37.26.146.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.8.204.58	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/igf	Block	2
37.26.146.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
192.118.78.198	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mains/sachar	Block	2
46.19.85.157	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
109.66.31.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Â	Block	2
180.191.103.179	Philippines	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
37.26.146.149	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
185.32.179.105	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
180.191.103.179	Philippines	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	2
109.253.218.152	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1403	Block	2
81.218.48.37	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	2
79.177.131.203	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation searchText in www.refua.atal.idf.il/1467-he/refuah.aspx	Block	2
2.54.150.54	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
82.210.20.27	Germany	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/wordpress/wp-admin/	Block	1
185.32.179.19	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.121.156.41	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
110.84.32.140	China	147.237.76.42	refuah.idf.il	Multiple Admin Blocking from 110.84.32.140	Block	1
109.253.203.120	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.178.28.134	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
169.229.3.91	United States	147.237.72.167	ishurim.aka.idf.i	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1